COPY.

POLISH CYPHERS 1942-1945

CODE BOOKS

During this period four Code Books have been used for Military Attache Telegrams, books 555, 666, 777 and 888. Book 555 seems to date from before the war. 666 was sent to Berne in May 1941 as a 'new book'. 777 was in use in the autumn of 1943. 888 was first used in September 1944. The most recent book was generally used, but not invariably - and at one time 555 and 666 were used by Berne for the same cypher with no indication at all as to which book was used. These books are all 4-Figure, with 10,000 groups, non-alphabetical.

We do not possess the Diplomatic Codebooks, of which there are at least two, known as 'Alpha' and '50'. (See TICOM article for German description: older book used for Consular, more recent for Dip. Traffic). TICOM/D-3n.).

MILITARY ATTACHE CYPHERS

I. Tables of Subtractor Groups.

A. In 1942 the olish Military Attaches relied almost entirely on this method. London distributed a series of these tables to outstations; the tables were in sets of about 3 pages, each page for use for 4 months. The sets were marked 'General' or 'Individual': 'general' tables were used for circular messages and for communications between outstations, 'individual' tables for communications between Central (i.e. London) and the outstations. Tables consisted of four-figure groups, usually about 20 lines of 30 columns, though the size of pages varied - sometimes square 25x25. Bigram indicators were placed all round the table, one bigram at each end of every line and column. In addition some tables were marked with a name or number e.g. 'FORD', '0749', which would be put at the beginning of each telegram. Then came the selected indicator either with the Bigram repeated E.G. 4242, making it obvious, or with two dummy figures after the indicator. The subtractor groups were then taken in order in the column or line reading away from the indicator - e.g. with an indicator on the bottom line of the table, the column of groups was taken from bottom to top : with an indicator on the right hand side of the table, the lime of groups was read from right to left (though individual groups were always read from left to right). At the end of the line or column, another indicator was taken as before etc..

B. Some improvements were introduced - sets of four tables for use at the same time irrespective of date, 3-Figure Indicators, followed with a dummy to make up a 4-Figure group, and tables of different sizes. As no check indicators were given at the end of each line or column of subtraction groups, it was very difficult to identify indicators without a considerable block of traffic. It is not known how long this system remained in use - probably it was still in use in June 1945 e.g. Stockholm 3434.

II. Subtractor Tables with Grill.

In 1944 the Grill System was introduced. Replacing the tables described above, the new system was used for almost all Military Attache traffic, until the London Polish Government came to an end in 1945. Attached to these notes will be found a Specimen Grill (in two forms marked A and B) and a subtractor table, all reduced in size for convenience - the Grills used in practice contained anything from 24 to 50 groups, the actual subtractor tables were about four times the size of the specimen one.

A. Tables.

(1) These were always issued in sets of 3 or (more recently)

4 pages. For the most part tables were 'individual' i.e. for the use of a single station for communications with London. A different set of tables was usually used for the answer traffic.

(2) The length of time a set of tables remained in use depended on the amount of traffic and presumably on the degree of security required. For the Berne-London traffic, tables were changed every three months.

(3) Subtraction figures were now in unbroken lines, no longer in 4-figure groups.

(4) On the top left hand side of the table, opposite each line is a bigram indicator (marked in RED on the example). This same column of indicators is repeated on the right hand edge of the table. Each table has about 33 lines. Where there are only 3 tables in a set, the lines can all be given different bigram numbers. When four tables (still of the same size) are used some of these bigrams will have to be used twice. These repeated bigrams will generally be found near the bottom of the table, for reasons to be explained later.

(5) There is a further set of indicators along the top of the table, by which each column can be designated by a bigram. The table is divided vertically into blocks of ten columns, starting from the left: the block on the extreme right may have less than ten columns. Each block has its own number (here marked in YELLOW), no number occurring more than once on any one table. The numbering of blocks is different on each page. The ten columns of each block are also numbered (here marked in BLUE). At first the numbering of columns was in normal order 1 2 3 4 or reversed 0 9 8 7: later it became usual to have unsystematic numbering though for some reason one block was always in numerical order. Any column of the table can thus be designated by a bigram- Yellow and Blue, in that order.

B. Grill.

(1) A grill was generally kept in use for about three months and was then replaced, at the same time as the subtractor tables. However on occasions the same grill was used for six months or more, with different sets of tables.

(2) The numbering of the holes of the grill gives the order in which the subtractor groups are to be taken. The numbering always follows some more or less regular route, (in the example it is a figure of eight).

(3) A common feature is the use of a grill in two different ways according to the direction of the traffic. Thus, for telegrams from Stockholm to London the grill will be used in the normal way - for telegrams from London to Stockholm the grill will be reversed i.e. turned back to front, and probably upside down as well. Each side of the grill will have its own markings of arrows and numbering of groups.

(4) The two arrows in the top left hand corner of the grill are used for setting it in any given position on the table. The arrows in the other three corners are used for checking this position (see below 'Indicators').

C. Indicators.

(1) Two 4-figure indicators groups are inserted in thettext for every setting of the grill. In order to identify these indicators it is necessary first to divide the text into 4-figure groups throughout, and then to mark it off into sections according to th

the length of the grill. For example, the specimen grill has 13 groups: there will be 2 indicator groups: thus each section will be 15 groups long. In each section of the telegram the first group will be the initial indicator, and the last group will be the check indicator. The last section of the telegram can be of any length from three to fifteen groups.

(2) The indicator groups have always been unconcealed.

(3) Initial Indicator. An example will make the use of the indicator clear. Suppose a telegram begins with the indicator group 0154. This must be considered as two bigrams 01 and 54. The first bigram 01 must be looked for among the left hand (RED) indicators on the tables and it will be necessary to look through the set of three or four tables to find on which table it occurs. Place the grill marked A on the required table so that the horizontal arrow in the top left hand corner is in line with the bigram 01 (in RED on the enclosed table). The second bigram 54 gives the indicator for the top of the table; 5 is the Block number (YELLOW) 4 is the column number (BLUE). Now, keeping the horizontal arrows aligned, slide the grill sideways until the vertical arrow in the top left hand corner points to the indicator 54. The grill is now in correct position , but this should be confirmed by the check indicator before the subtraction groups are taken.

(4) Check Indicator. To continue with the same example, we keep the grill A in the position described. The check indicator, the last group of the section, is 7172. As before, this is split into two bigrams. The first, 71, is found in column of RED indicators on the left of the table, opposite the horizontal arrows in the bottom corners of Grill A. The second bigram 72 has to be found at the top of the table (YELLOW and BLUE) and this proves to be in line with the vertical arrows in the right hand corners of the grill. Thus the setting of the gril is confirmed and the 13 subtractor groups can be taken.

There are in fact three possible check indicators that could be used for the initial indicator '0154', according to which pair of arrows is taken. '7172' is given by the bottom right hand corner, the check most frequently used in practice. The bottom left arrows give 7154, the top right 0172 : in each of these a bigram of the original indicator is repeated, a feature which is useful in identifying indicators. Note that this feature disappears when the grill is irregular in shape. Grill A is rectangular, with arrows symmetrically placed so that, for instance, the top horizontal arrows have the same alignment. Grill B has exactly the same spacing of groups, but the whole is irregularly shaped so that the arrows all have different alignment - thus the initial indicator 0154 with Grill B produces these three possible checks:- 3335, 4834, 4271, with no bigrams repeated. In practice, with irregular grills all three check indicators are used indiscriminately.

(5) For encyphering, it is simply necessary to choose the indicator, place the grill, construct the check indicator and insert the two indicators in the appropriate places in the text. It is obvious that with careful use many settings of the grill can be made without repeating an indicator or giving a depth. With a subtractor table of 33 lines, each of 75 digits (the usual size) and with a grill 11 lines deep and 21 digits wide, there are 1265 possible settings of the grill. Moreover, three or four of such tables are used together as a set.

(6) Where a set of four tables is used some of the left hand (RED) bigram indicators will occur twice. Most of these repeated bigrams will be found near the bottom of the column, too low down to be used as initial indicators. Where there is a choice of two tables, the check indicator will show which one is correct.

(7) It is not necessary to keep to any one table for encyphering a telegram.

Notes on Solution of Grill System.

(1) Identify the indicators and check groups,.

(2) Take each table separately - work out width and depth of the grill and from this the order of bigram indicators from the top and side - the block numbers (YELLOW) will give no difficulty, but the may not be possible to fill in all the column numbers (BLUE) until the table is reconstructed. The side order may prove difficult unless the encypherer has moved the grill regularly e.g. moving down one line for each indicator. Check indicators given by an irregular grill (see above) prove confusing at first, but are really a help, as theyconfirm the relative position of several bigrams - whereas a regular grill gives only the relativeposition of one pair of bigrams.

(3) Sections of telegrams with the same indicator are written out in depth, key breaking, differencing etc..

(4) When a number of groups have been broken on indicators lying close together on the table, look for the same subtractor groups appearing in two different indicators. When this is found, two holes can be cut in the grill, the first at random, the second placed in relation to the first. All subsequent holes must, of course, be cut in the same relation: adjustments can be made lated. Subtractor groups are filled in on the table as soon as the position of groups is known. Grill and table with luck will help each other. It may be necessary to look for repeated cypher text groups occurring in neighbouring indicators, though most of these repeats will be accidental: a machine could be used for finding them (as by the Germans). When the grill is complete reconstruct the table by key breaking. Much can be done with staggered depths and 'depths' of one when part of the subtractor is known.

(5) It is clear that nothing can be done untilthe order of the bigram indicators on the side and top of the table are reconstructed, and to do so it may be necessary to have a considerable volume of traffic. Much depends on the skill of the encypherer. Without repeated indicators, chances are slight.

(6) A large grill of, say, 48 groups is in practice very much more difficultto to break than a small one - partly because fewer indicators would be used.

(7) It proved very difficult to reconstruct the top order of the table in a line of traffic in which the 2nd bigram of the indicator was repeated in the check indicator i.e. the arrows in the bottom left hand corner of Grill A were always used. If unconcealed indicators are to be used, it would probably be an improvement simply to repeat the initial indicator instead of a check indicator.

DIPLOMATIC AND CONSULAR CYPHERS.

(1) Cypher "Z".
Letter cypher, simple transposition. The first two letters give the size of the cage, A=4, B=5, C=6 etc. Written downwards and read straight across. Used mainly for lowgrade routine matters, but some telegrams have been of considerable interest.

(2) Diplomatic Cypher in use before 1943 - see German essay TICOM/D-3m.

(3) Later Diplomatic Cypher:-
a) Letter 1943-4. Method unknown.
b) Figure 1944-5. 2nd and 3rd groups added together \gavedate and number. Method unknown.

POLISH MINISTRY OF INTERIOR CYPHERS.

The cypher here described was used between London and Vatican City from January 1945 onwards. The same system was probably used in several other lines of traffic.

(1) Traffic was sent in five figure groups.

(2) The last group of the telegram contained a three figure discriminant '396'. This could occur in any position in the group.

(3) The ninth five figure group of the telegam was an indicator, all five figures being significant. Telegrams with the same indicator were all encyphered similarly; but the difference of a single digit in the indicator meant a completely different encypherment.

(4) Each indicator referred to a particular key, which was probably taken from a prepared list or book. It was not derived mathematically from the indicator. The key consisted of a strip of about 40 figures; the length varied considerably and it was not necessarily an even number.

(5) For decyphering a telegram, the key was first used as a subtractor, repeating it as often as necessary.

(6) The first ten digits of the key were then used as the coordinates of a substitution square. The same square, 10x10, was used for all telegrams with the discriminent '396'. The square contained two complete alphabets, punctuation marks, the ten digits, some common bigrams (e.g. CZ, RZ, SZ), and repeats of the common letters - e.g. E occurs 5 times.

(7) The text resulting from the substraction was split into bigrams which were then converted by means of the substitution square.

(8) It is clear that as the first ten digits of the key were used as coordinates of the square, there could be no repeated digit. This proved an important limitation.

POLISH MILITARY CYPHERS.

Very little is known on this subject, but it is believed that the Poles made use of:-

(1) A 10x10 substitution square: the coordinates were taken from strips of about 20 figures which were used as slides, the settings being frequently changed.

(2) A slide whereby three figure groups were converted into pairs of letters.

(3) Subtractor tables - possibly with grill.

(4) Double transposition.

(5) One time pad.